PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	10/796,599
Filing Date:	March 9, 2004
Applicant:	Weishi Feng
Group Art Unit:	2132
Examiner:	Martin Jeriko P. San Juan
Title:	SECURE DIGITAL CONTENT DISTRIBUTION SYSTEM AND SECURE HARD DRIVE
Attorney Docket:	MP0386

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Claims 1-83 now are pending in the application. Claims 1-21, 23-79, and 81-83 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sims III (U.S. Pat. No. 6,550,011 B1) in view of Tai et al. (U.S. Pat. No. 2004/0034785A1).

Claim 1 recites the decryption of an encrypted content key using a private key that is generated based on a device specific identification (ID). The private key is used by a public key decryption module to decrypt an encrypted content key. Note that the private key is not used to decrypt encrypted content, but

rather is used to provide a content key for such decryption. Sims III and Tai fail to show, teach or suggest the stated decryption.

As Claim 1 recites a public key decryption module for a hard-disk drive that encrypts a content key, Claim 1 is directed to distributed content. In a distributed content environment, the content is encrypted by a distributor prior to reception by end users. The end users decrypt the content based on a received content key and a public/private key combination.

Traditionally, hard drives that are similar to each other may have or have access to the same private/public key sets. Thus, for example, should a storage medium such as a disk (platter) be removed from a hard drive, another hard drive may be able to decrypt information on that disk. The invention of Claim 1 prevents such access and limits decryption of content on a disk to only an individual hard drive with the device specific ID.

The Examiner admits that Sims III fails to disclose a private key that is generated based on a device specific ID. For at least this reason, Sims III also fails to disclose decryption of an encrypted content key using a private key that is generated via a device specific ID.

In an attempt to make up for the deficiencies in Sims III, the Examiner alleges that Tai discloses a private key that is generated via a device specific ID. The Examiner further alleges that the keys of Sims III and Tai are cryptographic keys and because of this it would have been obvious to generate the device specific key of Sims III using the private key generation technique of Tai. Applicant respectfully traverses and submits that the private key of Tai is

substantially different and is used differently than the device secret key of Sims III and the private key of Claim 1. Thus, it would not have been obvious to combine the relied upon references as suggested.

As best understood by Applicant, Sims III is directed to security of distributed content. The device secret key of Sims III is used to decrypt a content key, which is in turn used to decrypt distributed content.

In contrast and as best understood by Applicant, Tai is directed to security of boot-up software that is transferred between memories of a device. Tai discloses a private key that is used to encrypt boot-up software of a device, not to decrypt a content key. The boot-up software is locally stored on the device and is not distributed. The device includes ROM and a controller with RAM. The boot-up software is stored in the ROM. Upon an initial power up of the controller at an end product manufacturing site, the boot-up software is downloaded from the ROM to the RAM. The controller encrypts the boot-up software using a 64-bit number that is based on a chip's die ID number. Once encrypted, the boot-up software is up-loaded and stored on the ROM for future use.

Thus, the boot-up software of Tai is encrypted at the manufacturing site and stored on the ROM prior to the corresponding computer system being delivered to an end user. Once the end user receives the computer system, the encrypted software is simply decrypted for use by the computer system.

Thus, this encryption of Tai is directed to boot-up software that is stored and that remains on an onboard memory of a device. Tai is not directed to content that is distributed over a network. For this reason, Tai does not use

content keys and/or private/public key combinations. Therefore, Tai does not disclose decryption of an encrypted content key using a private key that is generated via a device specific ID.

Since there is no operative relationship between the device secret key of Sims III and the private key of Tai, there would be no reason to combine and/or modify the decryption techniques of Sims III using the private key encryption of Tai. In Sims III, the content key is distributed to multiple end users and the device secret key is used to decrypt a content key, not to encrypt distributed content. In Tai, the boot-up software is locally and internally encrypted via the private key. The boot-up software is not distributed, provided to multiple end users, or used for the decryption of a content key. Thus, the protection techniques and applications of Sims III and Tai are substantially different.

Also, Applicant further submits that cryptography is a very broad area. Cryptography is used in various mathematic, computer science, and engineering applications. The mere suggestion that the references can be combined based simply placing the references within the field of cryptography falls far short of the **explicit analysis** that is required by the Supreme Court in *KSR Int'l v. Teleflex Inc.*, 550 U.S. ____ (2007). Absent such an express teaching or suggestion in the references, the explicit analysis and reasoning must be supplied by the Examiner. *Id.* In other words, the Examiner is required to provide explicit reasoning as to why one skilled in the art would be motivated to decrypt a content key using a private key that is generated based on a device specific ID. Here, the Examiner merely notes that it would have been obvious "to generate

the device specific key of Sims III using the private key generation technique of Tai" and fails to provide explicit analysis and reasoning as required.

Furthermore, one cannot simply replace the device secret key of Sims III with the private key of Tai, as the keys are used differently. The private key of Tai is used for encryption of boot-up software and the device secret key of Sims III is used for the decryption of an encrypted content key. Thus, it is improper to combine the teachings of Sims III and Tai, as suggested.

It is a longstanding rule that to establish a prima facie case of obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 180 USPQ 143 (CCPA 1974), see M.P.E.P. §2143.03.

Therefore, Claim 1 is allowable for at least the above reasons. Claims 20, 31, 50 and 61 are allowable for at least similar reasons. Claims 2-19, 21-30, 32-49, 51-60 and 62-83 ultimately depend from Claims 1, 20, 31, 50 and 61 and are allowable for at least similar reasons.

Accordingly, Applicant respectfully submits that the pending claims are in a condition for allowance.

Respectfully submitted,

Dated: January 14, 2008

By: _____
Michael D. Wiggins
Reg. No. 34,754

Jeffrey J. Chapp
Reg. No. 50,579

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

MDW/JJC